Abstract

A method, system, and computer program product for the automatic detection and fixing of security vulnerabilities in both individual software components and across complex, multi-component software solutions. The architecture of the software solution to be monitored is analyzed prior to its being monitored. Data derived from the analysis is used to proactively identify possible ways to attack the software solution. The software solution being monitored and the system on which it runs is periodically scanned, and attacks on it are attempted. A list of possible attacks is continuously updated, for example, in a manner similar to virus signatures provided by virus security companies, and a log is generated describing which attacks were successful and which ones failed.